REMARKS/ARGUMENTS

The Applicant originally submitted Claims 1-14 in the application. In the present response, the Applicant has amended Claims 9-12 and added dependent Claims 15-16. Accordingly, Claims 1-16 are currently pending in the application. Support for the amendment can be found, for example, in paragraphs 14 and 56-76 of the original specification.

I. Rejection of Claims 9-12 under 35 U.S.C. §102

The Examiner has rejected Claims 9-12 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0016823 to Chung. The Applicant respectfully disagrees in view of amended independent Claim 9.

While Chung mentions an initial permutation for a Data Encryption Standard system used in block ciphering (*see* paragraphs 11, 17, 24 and Figure 2), the Applicant fails to find where Chung discloses defining a permutation source and padding a permuted message with the permutation source to obtain a preprocessed message as recited in amended independent Claim 9. On the contrary, Chung is concerned with encrypting and using irrational numbers as random numbers and irrational number generators as encryption processes for cryptographic applications. (*See* paragraph 32.) Thus, Chung is directed to encrypting but fails to disclose the preprocessing of a message before encrypting as recited in amended Claim 9.

Therefore, Chung does not disclose each and every element of amended independent Claim 9. As such, Chung does not anticipate Claim 9 and Claims 10-12 which depend thereon. Accordingly, the Applicant respectfully requests the Examiner to withdraw the §102 rejection with respect to Claims 9-12. Additionally, the Applicant fails to find where Chung anticipates new Claims 15-16.

II. Rejection of Claims 13 and 14 under 35 U.S.C. §102

The Examiner has rejected Claims 13 and 14 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,901,145 to Bohannon, *et al.* The Applicant respectfully disagrees.

Bohannon relates to the generation of a repeatable cryptographic key based on potentially varying parameters which are received. (*See* column 2, lines 38-41.) Bohannon does not teach, however, "computing the determinant of a matrix-based encrypted message matrix" as recited in independent Claim 13. Instead, Bohannon discloses computing the determinant of **cryptographic shares** to provide a secret key. (*See* column 10, lines 64-67.) The cryptographic shares are not an encrypted message matrix but are, for example, points on a polynomial that are used to identify a key. (See column 3, lines 17-30.) As such, Bohannon does not teach each element of Claim 13.

Since, Bohannon does not disclose each and every element of independent Claim 13, Bohannon does not anticipate Claim 13 and Claim 14 which depends thereon. Accordingly, the Applicant respectfully requests the Examiner to withdraw the §102 rejection with respect to Claims 13-14 and allow issuance thereof.

III. Rejection of Claims 1-8 under 35 U.S.C. §103

The Examiner has rejected Claims 1-8 under 35 U.S.C. §103(a) as being unpatentable over Bohannon in view of U.S. Patent Application Publication No. 2004/0062390 to Slavin. The Applicant respectfully disagrees.

The Examiner recognizes Bohannon does not teach or suggest "partitioning an input message into matrix elements." The Applicant also fails to find where Bohannon teaches or suggests "computing the determinant of said matrix," as asserted by the Examiner. (*See* Examiner's Action, page 4, citing column 10, line 64, to column 11, line 61, of Bohannon.) On the contrary, instead of computing the determinant of a matrix, wherein the matrix has elements of a partitioned input message, Bohannon discloses determining the determinant of a matrix of cryptographic shares to compute a secret key k. (*See* column 10, lines 64-67.) The cryptographic shares are not from a partitioned input message but are, for example, points on a polynomial that are used to identify a key. (*See* column 3, lines 17-30.)

Additionally, even assuming *arguendo* that computing the secret key k does disclose computing the determinant of a matrix as recited in Claim 1, Bohannon does not teach or suggest encrypting the secret key k. Instead, Bohannon teaches using the secret key k to encrypt cryptographic shares. (*See* column 3, lines 54-57, and column 11, lines 57-60.) Thus, Bohannon does not teach or suggest "encrypting said determinant" as recited in Claim 1. As such, Bohannon also fails to teach or suggest "multiplying said matrix by said encrypted determinant" as recited in Claim 1. Bohannon, therefore, does not teach or suggest each element for which it has been cited.

Slavin relates to cryptography for secure data transmission. (*See* paragraph 1.) Slavin has not been cited to cure the above noted deficiencies of Bohannon but to teach "partitioning an input message into matrix elements." (*See* Examiner's Action, pages 4-5.) The cited combination, therefore, of Slavin and Bohannon does not provide a *prima facie* case of obviousness of independent Claim 1 and Claims dependent thereon. The Applicant therefore respectfully requests the Examiner withdraw the §103(a) rejection of Claims 1-8 and allow issuance thereof.

IV. Conclusion

In view of the foregoing amendment and remarks, the Applicant now sees all of the Claims currently pending in this application to be in condition for allowance and therefore earnestly solicits a Notice of Allowance for Claims 1-16.

The Applicant requests the Examiner to telephone the undersigned attorney of record at (972) 480-8800 if such would further or expedite the prosecution of the present application. The Commissioner is hereby authorized to charge any fees, credits or overpayments to Deposit Account 08-2395.

Respectfully submitted,

HITT GAINES, PC

J. Joel Justiss
J. Joel Justiss
Registration No. 48,981

Dated: January 21, 2008

P.O. Box 832570
Richardson, Texas 75083
(972) 480-8800